Presentation to the SITAC Meeting

December 9, 2013

Brynhild Haugland Room

State Capitol Building

Agenda

Time

Time		
1:00	Welcome / Opening Comments	Mike Ressler
1:05	EA Waivers and Standards	Jeff Quast
1:15	Application Security (AppScan)	Dan Sipes
1:40	Data Breach Process	Mike Ressler
1:50	Disaster Recovery	Dan Sipes
2:00	BREAK	
2:10	FirstNet	Duane Schell
2:20	Business Analysis	Mike Ressler
2:30	Secretary of State Project	Al Jaeger / Mike Ressler
2:40	WSI Project	Clare Carlson
2:50	Open Discussion / Closing Comments	Mike Ressler

Mike Ressler

Welcome / Opening Comments

Introductions

Jeff Quast, Program Administrator

Enterprise Architecture

EA Requests for Exemption

- DOT requested an exemption from the Web Development Standard for a .com domain name

  - Request was denied

EA Standards

- Updated the Web Development Standard
  - Addresses things like HTML5 and CSS3

- Updated the Server Operating System Standard
  - Addresses modern architectures and platforms

- Rescinded the Document Management Workflow Standard
  - Was not applicable to actually defining workflow

Questions?

Thanks

Dan Sipes
Deputy CIO

Application Security – AppScan

- Security testing to determine application vulnerabilities in order to protect sensitive data.

    - Injection flaws occur when untrusted data is sent to an application as part of a command or query.

    - Cross site scripting (XSS) flaws occur whenever an application takes untrusted data and sends unintended content to a web browser.

AppScan – Application Assessment

- ITD uses a threat matrix assess application risk.
  - The threat matrix takes into account the presence of Personally Identifiable Information (PII):
    - Name, Address, Date of Birth
      Social Security Number
      Drivers License Number
      Credit Card Numbers

- ITD written Java applications are the focus during this initial stage, ITD written .NET applications and vendor applications will be included as future scope.

Application Security – AppScan

- Existing applications will be scanned according to a threat assessment priority.

- New applications will be scanned as part of ITD's software development lifecycle process.

- Plan to establish the application rescan process to address new vulnerabilities. Application risk assessment will be a contributing factor in determining rescan frequency.

AppScan – Discovery and Remediation

- Prior to the application scan, there will be a meeting with the Agency to discuss the discovery and remediation process in more detail

- Software Development Team Leader is the primary point of contact with ITD.

- The Agency and ITD will work together to finalize the remediation plan.

AppScan – Discovery and Remediation

- In the event the vulnerability is of high risk and is easily exploitable:
  - ITD will escalate the issue to the Agency contact through the Software Development Team Leader.
  - ITD's security incident management process will be initiated.
  - Mitigate the vulnerability and remediate the application code.

- Reviewing ITD processes as part of the current ManTech Audit.

Data Breach Process

Mike Ressler

Data Breach Process

- If agency is notified of possible data breach: contact ITD at 328-4470 (report security incident) and contact your attorney at AG's Office

- If ITD determines a possible data breach has occurred: we will contact the department director; Attorney General's office, Risk Management, and Governor's office

- Investigation will be conducted and department director will determine the need to communicate to the individuals possibly affected

Dan Sipes
Deputy CIO

IT Business Continuity Dependencies

SYSTEMS & DATA

NETWORK SERVICES

POWER & ENVIRONMENTALS

FACILITIES & STAFF

Disaster Recovery

- Background Information
    - **Recovery Point Objective (RPO):** The point in time to which data can be recovered when a disaster occurs. RPO refers to the time of the last successful data replication or backup. It focuses on data; it is independent of the time it takes to get non-functional system components back on-line.
    - **Recovery Time Objective (RTO):** A measure of how long it takes for a system to resume operations after a disaster has been declared.
    - http://www.nd.gov/itd/support/service-level-agreements
    - Enterprise SLA – RTO/RPO and Disaster Declaration (pages 7-8)
    - Hosting SLA – Data Backup and System Recovery (pages 3-4)

Disaster Recovery

- A limited subset of ITD hosting services have been architected for business continuity within their base rates.
  - Email, File/Print, Basic Phone Services – one hour RTO
  - Mainframe and ConnectND – twelve hour RTO

- Agencies are responsible for their data & applications
  - Coordinate with ITD for specific application RTO's

- Staffing constraints currently impact the amount of DR testing that can be accomplished. Minimum of three month lead time to get on the schedule for DR testing.

Break

Duane Schell
Director

Network Services Division

FirstNet™

VISION

To provide emergency responders with the first nationwide, high-speed, wireless broadband network dedicated to public safety

Background

- Born out of the 9/11 Commission report recommendations

- Part of the Middle Class Tax Relief and Job Creation Act (Feb 2012)

- Established the First Responder Network Authority

What is Firstnet

- Nationwide wireless data network for public safety
  - Think "4G" for public safety

- Provides additional features commercial networks do not provide:
  - Increased reliability
  - Priority and pre-emption
  - Dedicated wireless spectrum

FirstNet™

North Dakota's Role

- State and Local Implementation Grant Program(SLIGP)
  - Governance and needs assessment
  - Education and outreach
  - Asset identification
  - Carrier network assessment
  - Technology utilization survey
- ND awarded $1.1M

FirstNet™

North Dakota's Role

- ITD and DES joint effort

- Coordinating grant activities with SIEC

- Program management via ITD

- Contractors enlisted to carry out planning activities

FirstNet™

Eventual Outcome

- Provide feedback to Firstnet Authority
- Firstnet will develop a network and business model
- ND must decide:
  - Opt In – Choose to use Firstnet network
  - Opt Out – Build their own network according to nationwide specification
- Firstnet will simply be another "carrier" to choose

Business Analysis

Mike Ressler

Business Analysis

- The practice of enabling change in an organizational context, by defining needs and recommending solutions that deliver value to stakeholders.

- Disciplined approach for introducing and managing change to organizations.
  - it is a structured way of recognizing, formalizing and implementing change

- Used to identify and articulate the need for change in how organizations work, and to facilitate that change.

Process

- Complete prior to budget request / cost estimating / RFP

- Business Analysis used to document
    - Business requirements
    - Business processes
    - Business needs, issues, and goals
    - Business process improvements

- Stakeholders better understand the business processes

Benefits

- Validate / verify that business needs are met to ensure agencies get what they need, not just what they want

- Better understanding of an agency business to assist in strategic planning

- Identifying business changes / improvements within a state agency

- Ensuring changes to the business are implemented effectively and efficiently

- Better process for identifying and managing business requirements

- Improve accuracy of budget estimate and schedule

Training

- Watermark Learning is the training provider

- Participating Agencies: WSI, BND, ITD, DHS, DOT, HP, JSND and Higher Ed

- 98 people have taken the Business Analysis Fundamentals class

- 51 people have completed the additional 6 course Business Analysis Certificate program. These courses consist of:
    - Consulting Skills to solve Business Problems
    - Eliciting Business Requirements
    - Planning and Managing Requirements
    - Facilitation Skills Workshop
    - Use Case Modeling (was replaced by Facilitation Skills Workshop)
    - Business Process Modeling

- Other BA classes taken
    - Business Process Improvement
    - Getting Started in Business Process Management

Secretary of State File 2.0 Project

Variance Report

Al Jaeger / Mike Ressler

Causal Factors

- Many more business requirements than anticipated in the budget estimate

- Business processes more complex than anticipated in the budget estimate

- Project team struggled to come to a shared understanding of the business processes

- Staffing (e.g., limited availability of experienced ITD technical resources, SOS resources spread thin, key knowledge confined to a few people)

Lessons Learned

- Projects should undergo analysis resulting in creation of thorough business process and requirements documentation (including process mapping) in order to establish a more accurate budget and schedule

- Time and cost estimates need to consider staff availability in a more realistic fashion

- Key knowledge should not be confined to a few resources

Recovery Strategy

- The team is taking time to re-analyze and re-estimate scope, schedule and cost efforts to complete the project

- Based on this information, a re-plan will be developed (target Jan. 2014)

- Additionally, funding strategies will be devised to account for changes in the re-plan

Workforce Safety & Insurance Project

Variance Report

Clare Carlson

Budget / Schedule Metrics

- Project was terminated prior to completion (i.e. no portion of the iVOS software was implemented)

- Project began December 2007 and was terminated December 2012

- Total of $17,813,289 was spent on the project

Causal Factors

- A software vendor that did not perform

- Multiple changes in WSI executive leadership

- Numerous delays in schedule leading to morale issues and "burn out"

Lessons Learned

Lesson: Manage vendor contracts to the letter, from the start of the engagement, while leveraging the experts available in procurement, legal, finance, IT and project management during negotiations and as soon as issues start to arise.

Impact: Managing contracts to the exact specifications defined in the contract and taking swift action when a breach occurs can limit potential losses in cases where vendor expertise or commitment proves lacking.   Over the past three years state staff has gained significant experience in procurement practices, negotiation, and contract management. Leveraging those resources will help WSI apply the latest strategies for success.

Lessons Learned

Lesson: For large projects, require full-time onsite commitment of some vendor resources.

Impact: Requiring the provision of full-time onsite personnel can provide enforceability of the vendor's stated resource commitment and maximize communication and timeliness of feedback. The average response time for e-mail in 2012 was 2.5 days, an increase of 14% over the previous year. There is only a 56% chance someone will answer an email within an hour and 89% chance they will answer it within 24 hours. (Barr, 2013) Voice mail is even worse with more than 30 percent of voice mail messages remaining unheard for three days or longer. (Teitell, 2009) These inherent delays in communications can quickly start causing project delays. By having key staff on site throughout the project and bringing in additional SMEs ["Subject Matter Experts"] as needed, WSI can minimize delays caused by communication.

Lessons Learned

Lesson: Assign project management responsibility for large IT projects to a qualified Project Management Professional (PMP) ® credentialed project manager with ND large IT project experience, providing unfettered access to project sponsors and executive leadership to ensure the use of the state's methodology.

Impact: Assigning a PMP- credentialed project manager as primary PM provides WSI an assurance that this key position has both knowledge of project management principles and a minimum of 4500 hours of experience. In addition the certification requires continuing education to remain certified so the PM can assure WSI that his/her skills have remained fresh. The state qualifications ensure the PM understands the unique requirements placed upon WSI by North Dakota Century Code.

By providing unfettered access to executive sponsorship and final authority over official project communications, WSI can help ensure neutrality and transparency in the face of day-to-day organizational pressures and politics.

Lessons Learned

Lesson: Leverage the ESC for the expertise they have gained from projects across all agencies and to share responsibility in difficult decisions.

Impact: Part of the value Executive Order 2011-20 and recent legislation (N.D.C.C. § 54-59-32) has provided is the assignment of key personnel to sit on ESCs across multiple agencies. This provides experience unparalleled in any single agency. Leveraging these ESC members' expertise can help prevent the need for an agency to go it alone in facing complex project issues, allowing WSI to utilize the knowledge gained in other large state IT projects.

Lessons Learned

Lesson: Invest in mapping and reorganizing of granular business processes at the onset of the project, basing project objectives on them and providing success criteria on enabling of those processes in early stage gates.

Impact: Having business process documentation generated before trying to obtain and implement a solution can provide objectivity during project execution. This documentation can help management separate legitimate concerns raised by business from negativity born of resistance to change or other subjective reasons. It also provides WSI with clear measurement points to validate the vendor's solution early and often. WSI will be better equipped to determine if they need to cancel a project much earlier in the project timeline.

Lessons Learned

Lesson: Formulate an Organizational Change Management strategy and provide early and consistent communication of change on all levels.

Impact: One of the classic failures of an IT project is the successful implementation of a software product that no one uses. Organizational Change Management efforts help ensure the vision for the project is unified, that staff are ready for change; that resistance is managed effectively and proactively, and that everyone knows how they will accomplish their job in the new environment.

Lessons Learned

Lesson: Executives: Be transparent and involved leaders during projects through increased daily contact with team members and the timely sharing of information, both inside and outside the agency.

Impact: Ongoing face-to-face involvement from executive leadership with stakeholders at all levels of a project can help maintain trust, direction, and morale even when opinions on direction may otherwise diverge. Executive leadership must show that they are hearing the business staff's opinions while also taking the responsibility for making decisions, selling those decisions throughout the organization, and setting the expectation that WSI staff will support those decisions. Involvement that is direct and personal provides the best chance for harmonizing these goals.

Lessons Learned

Lesson: While fostering a culture within the project in which contrary views can be voiced, insist that such views be presented respectfully and with objective reasons. Deal immediately and consistently with behavior that crosses into the realm of obstructive or unprofessional. Remove repeat offenders from project roles to prevent damage to morale and objectives.

Impact: One of the core skills taught in a facilitation course is how to handle dysfunctional behavior. If it is not addressed, dysfunctional behavior tends to get worse over time. Left unchecked, it can spread to other members of the group. By fostering an environment that allows people to fully discuss their concerns and issues, WSI can avoid most disagreements. By addressing the higher-level disagreement quickly WSI can minimize dysfunctional behavior and prevent the behavior from spreading to other project members.

Lessons Learned

Lesson: Allow additional lead-time for planning and fulfillment of project resource needs in recognition of growing agency demands. Plan and budget for temporary staff to fill low-level positions to allow more experienced staff to step up to fill gaps left by people assigned to the project.

Impact: Estimating and analyzing expected resource allocation requirements for internal WSI staffing prior to product acquisition and execution can help the agency devise strategies to manage the strain of the project implementation.

One key strategy should be to plan for temporary staff to help fill gaps. This may require more than a one-for-one replacement to overcome lower efficiencies. WSI should bring the temporary staff on-board prior to project staff leaving in order to cover the training period

Lessons Learned

Lesson: Avoid solutions involving significant modification of COTS products as such approaches signal a likely mismatch to needs.

Impact: Solutions to project requirements that are dependent upon significant modification of commercial off-the-shelf (COTS) software are a red flag indicator of a potential mismatch with needs. Rather, WSI should make the selection of COTS solutions with the assumption that business units will need to modify their processes to fit the software. A key part of that analysis is identifying what functionality the business units would lose in a proposed system. Otherwise, WSI should consider a custom-developed solution or an approach involving customization of a framework intended for such modification.

Open Discussion

Closing Comments